VOLUNTARY UNDERTAKING UNDER
SECTION 48L OF THE PERSONAL DATA PROTECTION ACT 2012

Case number: DP-2308-C1305

In the matter of an investigation under section 50(1)

of the Personal Data Protection Act 2012 ("the Act")

And

(1) Low Keng Huat (Singapore) Limited (UEN No. 196900209G)

… Organisation

The Commission has reasonable grounds to believe that the Organisation has not complied, is not complying or is likely not to comply with section 24 of the Act. In order for the Commission to suspend its investigation pursuant to section 50(3)(ca) of the Act, the Organisation HEREBY UNDERTAKES that it will:

(a) Complete the remediation plan set out at Schedule B within the timelines stated in Schedule B; and

(b) Within 14 days of the completion of the remediation plan set out at Schedule B, provide the Commission with a copy of the declaration set out at Schedule C duly signed by the signatory of this Undertaking or a representative of the Organisation of equal designation.

The Organisation acknowledges that the Commission shall be entitled to publish and make available to the public this Undertaking and the summary of the Commission's findings set out at Schedule A to this Undertaking.

The terms of this Undertaking may be varied by the written agreement of the Commission and the Organisation.

SIGNED, for and on behalf of)

Low Keng Huat (Singapore) Limited)

By the following:)

Name: _____)

Designation: _____)

Date: _____)

SCHEDULE A

SUMMARY OF FACTS

1. On 31 July 2023, PDPC was notified by Low Keng Huat (Singapore) Limited ("**LKHS**") of a data security incident on 4 July 2023 involving ransomware encryption and possibly data exfiltration. LKHS staff had reported being unable to access the Organisation's workstations.

2. As a result, the personal data of 1,400 individuals including their names, addresses, personal email addresses, telephone numbers, NRIC numbers, passport numbers, photographs, dates of birth, transaction information was affected.

3. To prevent a recurrence of a similar incident, the Organisation took immediate remedial action to address the cause of the personal data breach.

SCHEDULE B

S/N	LIKELY CAUSES OF INCIDENT	PROPOSED STEPS TO ADDRESS THE CAUSE	TARGETED COMPLETION DATE
Tightened Governance over Outsourced Vendors and Infrastructure			
1.	Unpatched software and outdated firmware	Review and enhance vendors' execution of patches for each Windows and non-Windows platform a. List all patches and firmware updates communicated and executed by vendors on stated date b. Physically check for evidence that such patches and updates are completed c. Research any other available patches and updates not covered by vendors	20 Oct 2023 Audit Frequency: **Monthly** (on a Friday after Microsoft "Patch Tuesday")
2.	Outdated and incomplete IT hardware and software asset lists	Review and enhance current asset management processes: a. Record and document any event(s) necessitating fresh review b. Review and update inventory	27 Oct 2023 Audit Frequency: **Event-driven** as

		list(s) where necessary c. Check list(s) with actual (sighted) physical items	defined or **Annually**, whichever is earlier.
3.	Breakdown of vendor management and account responsibilities processes	Review and enhance vendors and account management process: a. Record and document any event(s) necessitating fresh review b. Review and update account management processes where necessary	20 Oct 2023 Audit Frequency: **Event-driven** as defined or **Annually**, whichever is earlier.
4.	Firewall not managed, absence of rules and log files monitoring	a. Record and document any event(s) necessitating fresh review b. Full firewall review: check rules, logs, bandwidth monitoring, list of super admin users, access security through Internet, logs monitoring, reporting frequency.	20 Oct 2023 Audit Frequency: **Event-driven** as defined or **Annually**, whichever is earlier.
	The immediate actions taken post incident had already fixed all firewall issues identified. We intend for another round of manual checks before the target completion date and provide		

	screenshots, log files as part of the status report at the end of the voluntary undertaking. In the event LKHS switches service provider, or changes the type of firewall used, we will repeat all the tasks as detailed in above.		
5.	VPN software end of life	Removed need for VPN, no longer using the VPN solution. Files and folders access via Microsoft Sharepoint.	N.A.
	Post incident, LKHS has discontinued the use of a VPN for external access to on-premise (local site) file servers. LKHS staff now use the public Internet to access files stored on Microsoft Sharepoint cloud. Existing local file servers (on-site) can be accessed only when physically in office, and using existing Active Directory credentials. LKHS has concluded there is no requirement to access any corporate work and assets from the Internet. The Management's decision is to use cloud Sharepoint as the main file access and sharing functionality without any need for a VPN. The previous VPN and local Active Directory security mechanism has been replaced with Microsoft's Azure Active Directory ("AAD") Authentication and Identity Management features. Authorised LKHS staff have been registered with the AAD and users need to sign in with their Azure AD credentials. Multi-factor authentication will be enforced as part of the LKHS remediation plan. LKHS uses Sharepoint's Role-Based Access Control (RBAC) to manage permissions and access. LKHS administrators will assign permissions to users and groups at various levels. Folder owners (designated staff) will need to grant privilege access to their respective team members, based on internal requirements.		
Cybersecurity Enhancements			
6.	Weak security settings for servers	Work with vendors to harden infrastructure using CIS benchmarks,	18 Oct 2023

		vendors' knowledge base or Windows Group Policy Objects	
7.	Lack of endpoint protection	Implement endpoint protection for all LKHS staff a. List all end users with and without endpoint antivirus software installed b. Monitor effectiveness and any expiry dates	31 Oct 2023
8.	Weak Microsoft account passwords, lack of 2FA	a. Implement Microsoft 2FA, password security and rules b. Review password policies and enforce strong password requirements	18 Oct 2023
9.	Lack of log file visibility and management	Monitor logs from key servers / firewall	27 Oct 2023
	Explore centralised log server to consolidate logs from key servers		

Staff Communication/Education and IT Policies				
S/N	**IDENTIFIED GAPS**	**AGENDA**	**MODE AND NEXT SCHEDULED DATE**	**SUBSEQUENT FREQUENCY**
1.	No schedule for staff communication	• Cybersecurity Training	Online or in person	Once per year

	and training on cybersecurity matters	• Training on LKHS IT Acceptable Use Policy	Within 1 month after remediation timeframe	Events when the policies are updated
2.	Lack of detail and actionable steps in current IT Policies Weak enforcement of policies related to IT Governance	• LKHS-IT-01 Vendor Management Policy • LKHS-IT-03 Acceptable Use Policy • IT Policy in Software and Patch Management	To extract and follow PDPC's Guides.	Once per year

SCHEDULE C

Case number: DP-2308-C1305

In the matter of an investigation under section 50(1)

of the Personal Data Protection Act 2012 ("the Act")

And

(1) Low Keng Huat (Singapore) Limited (UEN No. 196900209G)

… Organisation

DECLARATION

I refer to the voluntary undertaking dated _____ given by the Organisation to the Personal Data Protection Commission pursuant to section 48L of the Act ("**the Undertaking**").

I declare that the remediation plan set out at Schedule B of the Undertaking has been completed.

I acknowledge that by making a false declaration or providing false or misleading information to the Personal Data Protection Commission, I may be prosecuted for offences under section 51(3)(c) of the Personal Data Protection Act 2012 and/or section 182 of the Penal Code 1871.

_____ _____

Signature Date

_____ _____

Name Designation